REMARKS

In the final Office Action, the Examiner rejects claims 1, 4, 5, 8-10, 12-14, 16, 19, and 20 under 35 U.S.C. § 102(a) and/or 102(e) as anticipated by SCHNEIER et al. (U.S. Patent Application Publication No. 2002/0087882); rejects claims 6, 15, and 21 under 35 U.S.C. § 103(a) as unpatenable over SCHNEIER et al. in view of JUDGE (U.S. Patent No. 6,941,467); and rejects claims 7 and 22 under 35 U.S.C. § 103(a) as unpatentable over SCHNEIER et al. in view of BATES et al. (U.S. Patent No. 6,785,732). Applicants respectfully traverse these rejections.[1] Claims 1, 4-10, 12-16, and 19-22 are pending.

Claims 1, 4, 5, 8-10, 12-14, 16, 19, and 20 stand rejected under 35 U.S.C. § 102(a) and/or 102(e) as allegedly anticipated by SCHNEIER et al. Applicants traverse this rejection.

Independent claim 1 recites a device that includes at least one interface configured to receive data transmitted via a network; a firewall configured to: receive data from the at least one interface, determine whether the data potentially contains malicious content, and identify first data in the received data that potentially contains malicious content; intrusion detection logic configured to: receive the first data, and generate report information based on the first data; and forwarding logic configured to: receive the report information, forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content; and forward the report information to a remote central management system when the report

[1] As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine reference, assertions as to dependent claims, etc.) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicants reserve the right to analyze and dispute such assertions/requirements in the future.

information indicates that the first data potentially contains malicious content, the report information allowing the remote central management system to make a forwarding decision on behalf of the device. SCHNEIER et al. does not disclose or suggest this combination of features.

For example, SCHNEIER et al. does not disclose or suggest forwarding logic configured to receive report information and forward first data for processing by a user application when the report information indicates that the first data does not contain malicious content. The Examiner relies on paragraph 0064 of SCHNEIER et al. as allegedly disclosing this feature (final Office Action, pg. 3). Applicants respectfully disagree with the Examiner's interpretation of SCHNEIER et al.

At paragraph 0064, SCHNEIER et al. discloses:

> FIG. 2 is a system overview of an exemplary embodiment of a probe/sentry system. One or more such systems can be installed at each customer site to monitor the customer's network and network components. (A database of all network components monitored by such probe/sentry systems may be stored by SOCRATES 6000 in a database similar to that suggested in TABLE 7 of Appendix C.) Data collected by sensors 1010, 1020, 1030 and 1040 (note that four sensors are shown solely by way of example and are not meant to limit the scope of the invention) are collated by sensor data collator 2010. Once collated, the data is first filtered by negative filtering subsystem 2020, which discards uninteresting information, and then by positive filtering subsystem 2030, which selects possibly interesting information and forwards it to communications and resource coordinator 2060. Data neither discarded by negative filtering subsystem 2020 nor selected out as interesting by positive filtering subsystem 2030 form the "residue," which is sent to anomaly engine 2050 for further analysis. Anomaly engine 2050 determines what residue information may be worthy of additional analysis and sends such information to communications and resource coordinator 2060 for forwarding to the SOC. Negative filtering, positive filtering, and residue analysis are examples of data discrimination analyses, other types of which are well-known to those skilled in the art.

This section of SCHNEIER et al. discloses a probe/sentry system that analyzes and acts on interesting data or anomalies by filtering data by a negative filtering subsystem to discard uninteresting information and then filtering the data by a positing filtering subsystem, which selects possibly interesting information and forwards it to a

communications and resource coordinator. Specifically, this section of SCHNEIER et al. discloses filtering and discarding uninteresting data (i.e. data the does not contain malicious content), This section of SCHNEIER et al. does not disclose or suggest forwarding logic configured to receive report information based on the data, as required by claim 1.

This section of SCHNEIER et al. further discloses sending "residue" (i.e. data neither discarded by the negative filtering subsystem nor selected out as interesting by the positing filtering subsystem) to an anomaly engine for further analysis. The "residue" of SCHNEIER et al. does not correspond to data that does not contain malicious content since the "residue" is the leftover data, not data that has been discarded by the negative filtering subsystem. Therefore, this section of SCHNEIER et al. does not disclose or suggest forwarding logic configured to receive report information and forward first data for processing by a user application when the report information indicates that the first data does not contain malicious content, as recited in claim 1.

Furthermore, as noted above, SCHNEIER et al. discloses discarding uninteresting data, and does not disclose or suggest forwarding the data for processing by a user application, as recited in claim 1. Therefore, this section of SCHNEIER et al. does not disclose or suggest forwarding logic configured to receive report information and forward first data for processing by a user application when the report information indicates that the first data does not contain malicious content, as recited in claim 1.

The Examiner alleges, on page 2 of the final Office Action, that "[t]he described functionality of Schneier occurs within a firewall system ([0034]-[0035]), wherein the firewall forwards legitimate traffic to the intended destination once the filtering

procedures have determined the traffic to be legitimate. This is how firewalls work. The portion of Schneier discussed by Applicant shows how the data representative of the traffic being examined is discarded once it has been determined that the traffic is non-malicious. At which point the legitimate traffic would be passed to the intended destination, otherwise absolutely nothing would pass the firewall." Applicants respectfully disagree with the Examiner's allegations regarding the disclosure of SCHNEIER et al.

At paragraphs 0034-0035, SCHNEIER et al. discloses:

> FIG. 1 is a overview of the systems in an MSM service exemplary implementation of the present invention. FIG. 1 is divided into two portions, components and systems that operate on the customer site (that is, within the customer's firewall) and components and systems that operate within the SOC (that is, within the SOC firewall). A single SOC can monitor and service multiple customer sites, and a single customer site can be monitored by multiple probe/sentry systems. For ease in understanding, this discussion assumes a single SOC servicing a single customer site being monitored by a single probe/sentry system.
>
> Probe/sentry system 2000, which can be implemented in software or hardware or a combination of software and hardware, monitors sensors attached to customer network 1000 for evidence of potential security-related events happening on network 1000. Such sensors can include firewalls and intrusion detection systems 1010, commercially available sensors and agents 1020, decoys and honeypots 1030 (monitored devices or programs specifically and solely designed to attract the attention of, and thereby expose, a would-be intruder), and custom sensors and agents 1040. More generally, probe/sentry system 2000 can monitor and collect information from any network component (whether software or hardware or a combination of both) that can be configured to send or provide to it status data (including audit log data and other audit information) concerning the status of network 1000 and its components.

This section of SCHNEIER et al. discloses a probe/sentry system that monitors sensors, such as firewalls, for evidence of potential security-related events happening on a network. This section of SCHNEIER et al. **does not disclose a firewall system**. Rather, this section of SCHNEIER et al. clearly states that the probe/sentry system can monitor and collect information from any network component that can be configured to send it status data concerning the status of the network and its components. In other words, the

probe/sentry system of SCHNEIER et al. can monitor a firewall and log data, such as suspicious activity. Therefore, as noted above, SCHNEIER et al. discloses discarding (i.e., not logging) uninteresting data, and does not disclose or even remotely suggest passing legitimate traffic to the intended destination, as alleged by the Examiner (final Office Action, pg. 2). Therefore, SCHNEIER et al. does not disclose or suggest forwarding logic configured to receive report information and forward first data for processing by a user application when the report information indicates that the first data does not contain malicious content, as recited in claim 1.

For at least the foregoing reason, Applicants submit that claim 1 is not anticipated by SCHNEIER et al.

Claims 4, 5, 8, and 9 depend from claim 1. Therefore, these claims are not anticipated by SCHNEIER et al. for at least the reasons given above with respect to claim 1.

Independent claims 10 and 16 recite features similar to, yet possibly of different scope than, features recited above with respect to claim 1. Therefore, Applicants submit that claims 10 and 16 are not anticipated by SCHNEIER et al. for at least reasons similar to the reasons given above with respect to claim 1.

Claims 12-14 depend from claim 10. Therefore, claims 12-14 are not anticipated by SCHNEIER et al. for at least the reasons given above with respect to claim 10.

Claims 19 and 20 depend from claim 16. Therefore, claims 19 and 20 are not anticipated by SCHNEIER et al. for at least the reasons given above with respect to claim 16.

Claims 6, 15, and 21 stand rejected under 35 U.S.C. § 103(a) as unpatentable over SCHNEIER et al. in view of JUDGE. Applicants respectfully traverse this rejection.

Claim 6 depends from claim 1, claim 15 depends from claim 10, and claim 21 depends from claim 16. Without acquiescing in the rejection of claims 6, 15, and 21, Applicants submit that the disclosure of JUDGE does not remedy the deficiencies in the disclosure of SCHNEIER et al. set forth above with respect to claims 1, 10, and 16. Therefore, claims 6, 15, and 21 are patentable over SCHNEIER et al. for at least the reasons given above with respect to claims 1, 10, and 16.

Claims 7 and 22 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over SCHNEIER et al. in view of BATES et al. Applicants respectfully traverse this rejection.

Claim 7 depends from claim 1 and claim 22 depends from claim 16. Without acquiescing in the rejection of claims 7 and 22, Applicants submit that the disclosure of BATES et al. does not remedy the deficiencies in the disclosure of SCHNEIER et al. set forth above with respect to claims 1 and 16. Therefore, claims 7 and 22 are patentable over SCHENIER et al. and BATES et al., whether taken alone or in any reasonable combination, for at least the reasons set forth above with respect to claims 1 and 16.

In view of the foregoing remarks, Applicants respectfully request withdrawal of the outstanding rejections and the timely allowance of this application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

By: /Meagan S. Walling, Reg. No. 60,112/
Meagan S. Walling
Reg. No. 60,112

Date: January 9, 2008

11350 Random Hill Road
Suite 600
Fairfax, VA 22030
(571) 432-0800

Customer Number: 25537